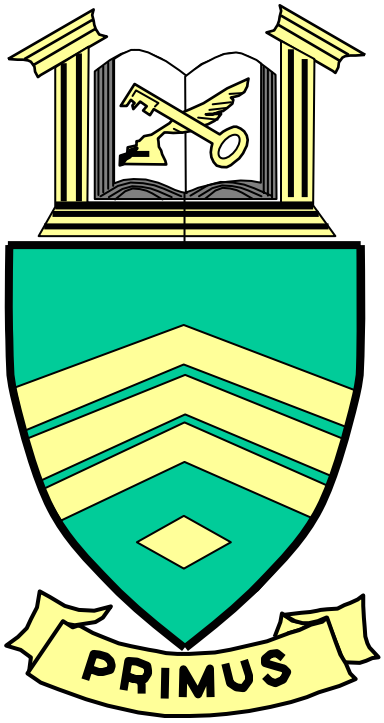
U.S. ARMY SERGEANTS MAJOR ACADEMY (FSC-TATS)

U652 (052002) JUN 01

THE ARMY PRIVACY PROGRAM

PRERESIDENT TRAINING SUPPORT PACKAGE LESSON



Overview

As a first sergeant, you can expect inquiries and/or requests for information on personnel assigned to your unit. Requests may come from other Army elements, other government agencies, the civilian business sector, or from private individuals. The handling and release of personal information is a sensitive issue and governed by law. This lesson will help you understand your administrative responsibilities and duties when you collect/maintain personal information on your soldiers and respond to inquiries concerning them. You must protect your soldier's rights from unwarranted invasion of privacy.

Inventory of Lesson Materials

Prior to starting this lesson, ensure you received all materials (pages) required for this Training Support Package. Go to the "**This [TSP or Appendix] Contains**" section, on page two of the TSP and the first page of each Appendix, and verify you have all the pages. If you are missing any material, contact the First Sergeant Course Class Coordinator at the training institution where you will attend phase II FSC-TATS.

Point of Contact

If you have any questions regarding this lesson, contact the First Sergeant Course Class Coordinator at the training institution where you will attend phase II FSC-TATS.

PRERESIDENT TRAINING SUPPORT PACKAGE

TSP Number /Title	U652 The Army Privacy Program
Effective date	JUN 01
Supersedes TSPs	U652, The Army Privacy Program OCT 00
TSP User	This TSP contains a training requirement that you must complete prior to attending phase II, FSC-TATS. It will take you about 1 hour to complete this requirement.
Proponent	The proponent for this document is the U.S. Army Sergeants Major Academy. POC: FSC-TATS Course Chief, DSN: 978-8329/8848; commercial: (915) 568-8329/8848.
Comments/ Recommen-dations	Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to: ATTN ATSS DCF FSC TATS COMDT USASMA BLDG 11291 BIGGS FLD FT BLISS TX 79918-8002
Foreign Disclosure Restrictions	The lesson developer in coordination with the USASMA foreign disclosure authority has reviewed this lesson. This lesson is releasable to foreign military students from all requesting foreign countries without restrictions.

This TSP Contains

The following table lists the material included in this TSP:

SECTION I, ADMINISTRATIVE DATA

Task Trained

This lesson trains the task listed in the following table:

Task number	121-010-8020
Task title	Supervise unit personnel and administration functions,
Conditions	You are a company level leader in a garrison or field environment responsible for the supervision of unit personnel and administrative functions,
Standards	Directs unit personnel and administrative functions IAW with prescribed publications/guidance.
Task proponent	Soldier Support Institute (SSI).

Task Reinforced/ Supported

None

Prerequisite Lesson

None

Clearance and Access

There is no clearance or access requirement for this lesson.

Copyright Statement

No copyrighted material reproduced for use in this lesson.

References

The following table lists the reference for this lesson:

Number	Title	Date	Para No.	Additional Information
AR 340-21	The Army Privacy Program	Jul 85		Chap 1 thru 4

Equipment Required

None

Materials Required

None

Safety Requirements

None

Risk Assessment Level

Low

Environmental Considerations

None

Lesson Approval The following individuals reviewed and approved this lesson for publication and incorporation into the First Sergeant Course--The Army Training System.

Name/Signature	Rank	Title	Date
Benjamin M. Salcido	GS9	Training Specialist	
Chris L. Adams	SGM	Chief Instructor, FSC	
John W. Mayo	SGM	Course Chief, FSC-TATS	

SECTION II INTRODUCTION

Terminal Learning Objective At the completion of this lesson, you will--

Action:	Determine unit level responsibilities under the Army Privacy Program,
Conditions:	as a first sergeant in a classroom environment, given an extract of AR 340-21 (SH-1),
Standard:	Determined unit level responsibilities under the Army Privacy Program IAW SH-1.

Evaluation Before entering phase II FSC-TATS, you will receive the end of Phase I Performance Examination that will include questions based on material in this lesson. On that examination, you must answer at least 70 percent of the questions correctly to achieve a GO.

Instructional Lead-in As First Sergeant, you will handle a variety of requests for information about your soldiers. You must know the policies and procedures that protect their privacy. In addition, you must know what information you may release and the rights of soldiers concerning information that the Army has collected on them.

SECTION III PRESENTATION

ELO 1

Action:	Identify Army policies and responsibilities under the Army Privacy Program,
Conditions:	as a first sergeant in a classroom environment, given SH-1,
Standard:	Identified Army policies and responsibilities under the Army Privacy Program IAW SH-1.

Learning step/ Activity (LS/A) 1, ELO 1

To complete the learning activity, you must--

- Read Chapter 1, AR 340-21, SH-1 at Appendix C.
- Complete questions 1 through 4 in lesson exercise 1 (Appendix B).
- Compare your responses with the solution found in the SLE-1.
- If your responses do not agree with the answer in the solution discussion, review the Student Handout.

ELO 2

Action:	Identify individual rights of access and amendment under the Privacy Act,
Conditions:	as a first sergeant in a classroom environment, given SH-1,
Standard:	Identified individual rights of access and amendment under the Privacy Act IAW SH-1.

LS/A 1, ELO 2

To complete the learning activity, you must--

- Read Chapter 2, AR 340-21, SH-1 at Appendix C.
- Complete questions 5 through 8 in lesson exercise 1 (Appendix B).
- Compare your responses with the solution found in the SLE-1.
- If your responses do not agree with the answer in the solution discussion, review the Student Handout.

ELO 3

Action:	Identify proper disclosure of personnel information to other agencies and third parties,
Conditions:	as a first sergeant in a classroom environment, given SH-1,
Standard:	Identified proper disclosure of personnel information to other agencies and third parties IAW SH-1.

LS/A 1, ELO 3 To complete the learning activity, you must--

- Read Chapter 3, AR 340-21, SH-1 at Appendix C.
- Complete questions 9 through 11 in lesson exercise 1 (Appendix B).
- Compare your responses with the solution found in the SLE-1.
- If your responses do not agree with the answer in the solution discussion, review the Student Handout.

ELO 4

Action:	Identify record keeping requirements under the Privacy Act,
Conditions:	as a first sergeant in a classroom environment, given SH-1,
Standard:	Identified record keeping requirements under the Privacy Act IAW SH-1.

LS/A 1, ELO 4 To complete the learning activity, you must--

- Read Chapter 4, AR 340-21, SH-1 at Appendix C.
- Complete questions 12 through 15 in lesson exercise 1 (Appendix B).
- Compare your responses with the solution found in the SLE-1.
- If your responses do not agree with the answer in the solution discussion, review the Student Handout.

SECTION IV SUMMARY

Review/ Summarize Lesson	As a First Sergeant, one of your responsibilities is protecting the privacy of your soldiers. You must guard against the unlawful collection, maintenance, and release of personal information concerning your soldiers. You must understand the Army Privacy Program and follow its guidance in performing your duties as First Sergeant. The Army Privacy Program relates to all areas of unit administration. It may be necessary to refer to AR 340-21 often as you perform your duties as First Sergeant. When you encounter questionable situations on the job, remember to check the regulation or call your Privacy Act Official for assistance.
Check on Learning	If your completed lesson exercises do not agree with the suggested solution, be sure to review the student handouts.
Transition to Next Lesson	None

SECTION V STUDENT EVALUATION

Testing Requirements	Before entering phase II FSC-TATS, you will receive the end of Phase I Performance Examination that will include questions based on material in this lesson. On that examination, you must answer at least 70 percent of the questions correctly to achieve a GO.

THIS PAGE INTENTIONALLY LEFT BLANK

SECTION VI QUESTIONNAIRE

Directions Complete the following actions:

- Enter your name, your rank, and the date you complete this questionnaire.

Name:	Rank:	Date:

- Answer items 1 through 6 below.
- Fold the questionnaire, so the address for USASMA is visible.
- Print your return address, add postage, and mail.

Note: Your response to this questionnaire will assist the Academy in refining and improving this course. When completing the questionnaire, answer each question frankly. Your assistance helps build and maintain the best curriculum possible.

Item 1	Do you feel you met the learning objectives of this lesson?
Item 2	Was the material covered in this lesson new to you?
Item 3	Which parts of this lesson were most helpful to you in learning the objectives?
Item 4	How could we improve the format of this lesson?
Item 5	How could we improve the content of this lesson?
Item 6	Do you have additional questions or comments? If you do, please list them here. You may add additional pages if necessary

ATTN ATSS DCF FSC TATS
COMDT USASMA
BLDG 11291 BIGGS FLD
FT BLISS TX 79918-8002

Appendix B

Index of Lesson Exercises and Solutions

This Appendix Contains

This Appendix contains the items listed in this table--

Lesson Exercise 1
The Army Privacy Program

Overview: As a first sergeant, one situation you can expect to encounter on a daily basis is the maintenance of, and request for information on the personnel assigned to your unit. Requests for such information may come from other Army elements, other government agencies, civilian businesses, or private individuals. The handling and release of personal information is a touchy area. This lesson will assist you in meeting your administrative responsibilities of collecting and maintaining personal information about your soldiers while protecting their legal rights and their privacy.

ELO 1: Identify Army policies and responsibilities under the Army Privacy Program. (Reference: AR 340-21, chapter 1)

The Army's policy on the Privacy Program permits you to collect personal information on personnel in your unit. However, the Army Privacy Program also requires those who keep records on individuals, to let those individuals (known as data subjects) know what records are on file. You must allow those individuals (or data subjects) to review or get copies of those records pertaining to them. AR 340-21 spells out Army policy on individuals' privacy rights and requirements established by the Privacy Act.

Item 1: As required by the Privacy Act of 1974 (and its amendments), the Army will protect the privacy of individuals from what?

Item 2: How does AR 340-21 define individuals protected under the Privacy Act?

Item 3: Under the Privacy Act, the Army permits you to only collect what kind of personal information about an individual?

Item 4: What requirements does the Army place on you under the Privacy Act regarding the personal information you may keep on an individual?

It is the responsibility of the Army, and you as an Army representative, to safeguard personal information to prevent unauthorized use, access, disclosure, alteration, or destruction.

AR 340-21 discusses access and amendment refusal authorities (AARAs). These AARAs are responsible for action on requests for access to, or amendment of records in their functional areas. For example, the Surgeon General is the AARA for medical records and the commanding General, U.S. Army Military Personnel Center is the AARA for personnel and personnel-related records of Active duty Army members.

ELO 2: Identify individual rights of access and amendment under the Privacy Act. (Reference: AR 340-21, chapter 2)

The Army's policy and responsibilities on the Privacy Act make it clear that individuals have rights of access to their records. Individuals or their representatives may request access to records that pertain to those individuals. They may make the request orally or in writing.

Item 5: What are two main exceptions that cause an individual to NOT receive access to their records?

AR 340-21, para 2.3, requires anyone receiving a request for access to records under the Privacy Act to also process the request as a Freedom of information Act (FOIA) request. This means that if the individual receiving the request for access denies furnishing all or any portion of the requested material, he must justify the denial under the substantive provisions of both the Privacy Act and the Freedom of Information Act. (For more information on FOIA see AR 25-55, The Department of the Army Freedom of Information Act Program.)

Item 6: If you work with medical records, you may need to make special considerations before releasing them. Carefully consider if the information could have an adverse effect on the mental or physical health of the individual. If this is a possibility, what does AR 340-21 advise you to do?

Item 7: Who are the only officials authorized to deny a request from an individual (data subject) for records pertaining to that individual?

If individuals believe their records are inaccurate, irrelevant, untimely, or incomplete, they may request the amendment of their records.

Item 8: If individuals believe their records need amendments, to whom should they address their requests to amend the records?

ELO 3: Identify proper disclosure of personnel information to other agencies and third parties. (Reference: AR 340-21, chapter 3.)

The Privacy Act prohibits the Army from disclosing personal information without obtaining prior written consent from the individual (data subject) concerned. However, there are numerous exceptions listed in AR 340-21 para 3.1.

Item 9: AR 340-21 indicates blanket routine uses, or situations when you may release information. Under what conditions may you refer Army records to Federal, State, local or foreign law enforcement agencies?

Item 10: You may disclose a record with what kind of information to OPM?

Under the Freedom of Information Act, you may release some personal information to third parties. Do not release lists of military personnel addresses or phone numbers for the purpose of commercial solicitation.

Item 11: What information on military personnel may you release under the Freedom of Information Act?

ELO 4: Identify record keeping requirements under the Privacy Act. (Reference: AR 340-21, chapter 4.)

You may keep personal notes and records on personnel in your unit. The Privacy Act does not consider your personal notes to be Army records. However, you must restrict your use of such notes to memory aids. Any disclosure from your personal notes, either intentional or through carelessness causes the notes to become subject to provisions of the Privacy Act.

Item 12: Whenever you request personal information from members of your unit for a system of records, you must furnish the individual with a Privacy Act Statement. What is the purpose of furnishing the Privacy Act Statement?

Item 13: The Army is authorized to use the SSN as a system to identify Army members and employees. What must an Army activity do if individuals refuse to disclose their SSN?

Item 14: The Privacy Act requires establishment of proper administrative, technical, and physical safeguards to ensure the security and confidentiality of records. These measures are to protect against what?

Item 15: If you violate provisions of the Privacy Act, you are subject to both civil and criminal penalties. An individual may file a civil suit against the Army if Army personnel fail to comply with the Privacy Act. What three willful actions by you would make you guilty of a misdemeanor and subject to fines under criminal penalties?

Solution/Discussion to Lesson Exercise 1
The Army Privacy Program

ELO 1: Identify Army policies and responsibilities under the Army Privacy Program.

Item 1: As required by the Privacy Act of 1974 (and its amendments), the Army will protect the privacy of individuals from what?

Unwarranted intrusion.

Reference: SH-1-2, AR 340-21, para 1.5a.

Item 2: How does AR 340-21 define individuals protected under the Privacy Act?

Living citizens of the United States and aliens lawfully admitted for permanent residence.

Reference: SH-1-2, AR 340-21, para 1.5a.

Item 3: Under the Privacy Act, the Army permits you to only collect what kind of personal information about an individual?

You may collect only that information that is legally authorized and necessary to support Army operations.

Reference: SH-1-2, AR 340-21, para 1.5b.

Item 4: What requirements does the Army place on you under the Privacy Act regarding the personal information you may keep on an individual?

Information you may keep on an individual must be timely, accurate, complete, and relevant to the purpose for which you collected it.

Reference: SH-1-2, AR 340-21, para 1.5c

ELO 2: Identify individual rights of access and amendment under the Privacy Act. (Reference: AR 340-21, chapter 2)

Item 5: What are two main exceptions that cause an individual to NOT receive access to their records?

- The record is subject to an exemption and the system manager has invoked the exemption.
- The record is information compiled in reasonable anticipation of a civil action or proceeding.

Reference: SH-1-2, AR 340-21, para 2.1a(1) and (2).

Item 6: If you work with medical records, you may need to make special considerations before releasing them. Carefully consider if the information could have an adverse effect on the mental or physical health of the individual. If this is a possibility, what does AR 340-21 advise you to do?

Ask the individual to name a physician to receive the record.

Reference: SH-1-4, AR 340-21, para 2.5.

Item 7: Who are the only officials authorized to deny a request from an individual (data subject) for records pertaining to that individual?

The appropriate access and amendment refusal authority (AARA), or the Secretary of the Army, acting through the General Counsel.

Reference: SH-1-4, AR 340-21, para 2.9a.

Item 8: If individuals believe their records need amendments, to whom should they address their requests to amend the records?

The custodian or system manager of the records.

Reference: SH-1-5, AR 340-21, para 2.11a

ELO 3: Identify proper disclosure of personnel information to other agencies and third parties. (Reference: AR 340-21, chapter 3.)

Item 9: AR 340-21 indicates blanket routine uses, or situations when you may release information. Under what conditions may you refer Army records to Federal, State, local or foreign law enforcement agencies?

If the record indicates a violation or potential violation of law and the requesting agency has the responsibility to investigate or prosecute the violation.

Reference: SH-1-6, AR 340-21, para 3.2a.

Item 10: You may disclose a record with what information to OPM?

Information on pay and leave, benefits, retirement deduction, and any other information necessary for OPM to carry out its legally authorized Government-wide personnel management functions and studies.

Reference: SH-1-7, AR 340-21, para 3.2h.

Item 11: What information on military personnel may you release under the Freedom of Information Act?

Name, rank, date of rank, gross salary, present and past duty assignments, future assignments that are officially established, office or duty telephone number, source of commission, promotion sequence number, awards and decorations, military and civilian educational level, and duty status at any given time.

Reference: SH-1-7, AR 340-21, para 3.3a(1).

ELO 4: Identify record keeping requirements under the Privacy Act. (Reference: AR 340-21, chapter 4)

Item 12: Whenever you request personal information from members of your unit for a system of records, you must furnish the individual with a Privacy Act Statement. What is the purpose of furnishing the Privacy Act Statement?

To ensure that individuals know why you are collecting the information so they can make an informed decision of whether or not to furnish it.

Reference: SH-1-8, AR 340-21, para 4.2a.

Item 13: The Army is authorized to use the SSN as a system to identify Army members and employees. What must an Army activity do if individuals refuse to disclose their SSN?

Identify the individuals by alternate means.

Reference: SH-1-8, AR 340-21, para 4.3.

Item 14: The Privacy Act requires establishment of proper administrative, technical, and physical safeguards to ensure the security and confidentiality of records. These measures are to protect against what?

Any threats of hazards to the subject's security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness.

Reference: SH-1-8, AR 340-21, para 4.4a(2).

Item 15: If you violate provisions of the Privacy Act, you are subject to both civil and criminal penalties. An individual may file a civil suit against the Army if Army personnel fail to comply with the Privacy Act. What three willful actions by you would make you guilty of a misdemeanor and subject to fines under criminal penalties?

- Maintaining a system of records without first meeting the public notice requirements of publishing in the Federal Register.
- Disclosing individually identifiable personal information to one not entitled to it.
- Asking for or getting another's record under false pretenses.

Reference: SH-1-9, AR 340-21, para 4.9b.

Appendix C

Index of Student Handouts

This Appendix Contains

This Appendix contains the items listed in this table--

Title/Synopsis	Pages
SH-1, Extract from AR 340-21, The Army Privacy Program, 5 July 1985	SH-1-1 thru SH-1-9

STUDENT HANDOUT 1

This Student Handout Contains

An extract from AR 340-21, The Army Privacy Program, 5 July 1985. We downloaded this extract from the U.S. Army Publishing Agency's web site at http://www-usappc.hoffman.army.mil/gils/epubs.html .
The extract may contain grammar errors and passive voice

Contents

NOTE: Figure 4.1 NOT included

Chapter 1
General Information

1.1 Purpose
This regulation sets forth policies and procedures that govern personal information kept by the Department of the Army (DA) in systems of records.

1.2. References
a. Required publications.
(1) AR 195-2, Criminal Investigation Activities. (Cited in para 2-10e.)
(2) AR 340-17, Release of Information and Records from Army Files. (Cited in paras 2-8 and 4-4c.)
(3) AR 340-21-8, The Army Privacy Program; System Notices and Exemption Rules for Civilian Personnel Functions. (Cited in para 2-9c.)
(4) AR 380-380, Automated Systems Security. (Cited in paras 4-b and 4-6c(8).)
b Related publications. (A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.)
(1) DODD 5400.11, DOD Privacy Program.
(2) DOD 5400.11-R, DOD Privacy Program.
(3) Treasury Fiscal Requirements Manual. This publication can be obtained from The Treasury Department, 15th and Pennsylvania Ave, NW, Washington, DC 20220.

1.3 Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in The glossary.

1.4 Responsibilities
a. The Assistant Chief of Staff for Information Management (ACSIM) is responsible for issuing policy and guidance for the Army Privacy Program In consultation with the Army General Counsel.
b. The Adjutant General (TAG) is responsible for developing and recommending policy to ACSIM concerning the Army Privacy Program and for overall execution of the program under the policy and guidance of ACSIM.
c. Heads of Army Staff agencies, field operating agencies, major Army commands (MACOMs), and subordinate commands are responsible for supervision and execution of the privacy program in functional areas and activities under their command.
d. Heads of Joint Service agencies or commands for which the Army is the Executive Agent, or otherwise has responsibility for providing fiscal, logistical, or administrative support, will adhere to the policies and procedures in this regulation.
e. Commander, Army and Air Force Exchange Service (AAFES), is responsible for the supervision and execution of the privacy program within that command pursuant to this regulation.

1.5 Policy
Army policy concerning the privacy rights of individuals and the Army's responsibilities for compliance with operational requirements established by the Privacy Act are as follows:
a. Protect, as required by the Privacy Act of 1974(5 USC 552a), as amended, the privacy of individuals from unwarranted intrusion. Individuals covered by this protection are living citizens of the United States and aliens lawfully admitted for permanent residence.
b. Collect only the personal information about an individual that is legally authorized and necessary to support Army operations. Disclose this information only as authorized by the Privacy Act and this regulation.
c. Keep only personal information that is timely, accurate, complete, and relevant to the purpose for which it was collected.
d. Safeguard personal information to prevent unauthorized use, access,
disclosure, alteration, or destruction.
e. Let individuals know what records the Army keeps on them and let them review or get copies of these records, subject to exemptions authorized by law and approved by the Secretary of the Army. (See chap 5.)
f. Permit individuals to amend records about themselves contained in Army systems of records, which they can prove are factually in error, not up-to-date, not complete, or not relevant.
g. Allow individuals to ask for an administrative review of decisions that deny them access to or the right to amend their records.
h. Maintain only information about an individual that is relevant and necessary for Army purposes required to be accomplished by statute or Executive Order.
i. Act on all requests promptly, accurately, and fairly.

1.6 Authority
The Privacy Act of 1974 (5 USC 552a), as amended, is the statutory basis for the Army Privacy Program. Within the Department of Defense (DOD), the Act is implemented by DODD 5400.11 and DOD 5400-11-R. The Act assigns--
a. Overall Government-wide responsibilities for implementation to the Office of Management and Budget (OMB).
b. Specific responsibilities to the Office of Personnel Management (OPM) and the General Services Administration (GSA).

1.7 Access and amendment refusal authority
Each access and amendment refusal authority (AARA) is responsible for action on requests for access to, or amendment of, records referred to them under this regulation. The officials listed below are the sole

AARAs for records in their functional areas:

a. The Adjutant General--for personnel records of Army retired, separated, and reserve military members; DOD dependent school student transcripts; and records not within the jurisdiction of another AARA.

b. The Administrative Assistant to the Secretary of the Army--for records of the Secretariat and its serviced activities, as well as those records requiring the personal attention of the Secretary of the Army.

c. The president or executive secretary of boards, councils, and similar bodies established by DA to consider personnel matters, excluding the Army Board for Correction of Military Records.

d. Chief of Chaplains--for ecclesiastical records.

e. Chief of Engineers--for records pertaining to civil works, including litigation; military construction; engineer procurement; other engineering matters not under the purview of another AARA; ecology; and contractor qualifications.

f. Comptroller of the Army--for financial records.

g. Deputy Chief of Staff for Personnel--for the records listed below.

(1) Personnel records of current Federal civilian employees and active and former nonappropriated fund employees(except those in the AAFES).

(2) Military police records.

(3) Prisoner confinement and correctional records.

(4) Safety records.

(5) Alcohol and drug abuse treatment records.

Note. (Requests from former civilian employees to amend a record in an OPM system of records such as the Official Personnel Folder should be sent to the Office of Personnel Management, Assistant Director for Workforce Information, Compliance and Investigations Group, 1900 E Street, NW, WASH DC 20415-0001.)

h. The Inspector General(TIG)--for TIG investigative records.

i. The Judge Advocate General (TJAG)--for legal records under TJAG responsibility.

j. The Surgeon General--for medical records, except those properly part of the Official Personnel Folder (OPM/GOVT-1 system of records).

k. Commander, AAFES--for records pertaining to employees, patrons, and other matters that are the responsibility of the Exchange Service.

l. Commanding General, U.S. Army Criminal Investigation Command (USACIDC)--for criminal investigation reports and military police reports included therein.

m. Commanding General, U.S. Army Intelligence and Security Command--for intelligence and security investigative records.

n. Commanding General, U.S. Army Materiel Command--for records of Army contractor personnel, exclusive of those in e above.

o. Commanding General, U.S. Army Military Personnel Center--for personnel and personnel-related records of Active duty Army members.

p. Commander, Military Traffic Management Command--for transportation records.

q. Chief, National Guard Bureau--for personnel records of the Army National Guard.

1.8 DA Privacy Review Board

The DA Privacy Review Board acts on behalf of the Secretary of the Army to decide appeals from refusal of the appropriate AARAs to amend records. Board membership is comprised of the Administrative Assistant to the Secretary of the Army, The Adjutant General, and The Judge Advocate General, or their representatives. The AARA may serve as a nonvoting member when the Board considers matters in the AARA's area of functional specialization. The Adjutant General chairs the Board and provides the Recording Secretary.

1.9 Privacy official

a. Heads of Army Staff agencies and commanders of MACOMs and subordinate commands and activities will designate a privacy official who will serve as a staff adviser on privacy matters. This function will not be assigned below battalion level.

b. The privacy official will insure that--

(1) Requests are processed promptly and responsively.

(2) Records subject to the Privacy Act in his or her command or agency are described properly by a published system notice.

(3) Privacy statements are included on forms and questionnaires that seek personal information from an individual.

(4) Procedures are in place to meet reporting requirements.

Chapter 2
Individual Rights of Access and Amendment

2.1 Access under the Privacy Act

a. Upon a written or oral request, an individual, or his or her designated agent or legal guardian, will be granted access to a record pertaining to that individual, maintained in a system of records, unless

(1) The record is subject to an exemption and the system manager has invoked the exemption(see chap 5), or

(2) The record is information compiled in reasonable anticipation of a civil action or proceeding.

b. The requester does not have to state a reason or justify the need to gain access. An individual cannot be denied access solely for refusal to provide his or her Social Security Number (SSN) unless the SSN was required for access by statute or regulation adopted prior to January

1, 1975. The request should be submitted to the custodian of the record.

2.2 Notifying the individual
The custodian of the record will acknowledge requests for access within 10 workdays of receipt. Releasable records will be provided within 30 days, excluding Saturdays, Sundays, and legal public holidays.

2.3 Relationship between the Privacy Act and the Freedom of Information Act
A Privacy Act request for access to records will be processed also as a Freedom of Information Act request. If all or any portion of the requested material is to be denied, it must be considered under the substantive provisions of both the Privacy Act and the Freedom of Information Act. Any withholding of information must be justified by asserting a legally applicable exemption in each Act.

2.4 Functional requests
If an individual asks for his or her record and does not cite or reasonably imply either the Privacy Act or the Freedom of Information Act, and another prescribing directive authorizes release, the records should be released under that directive. Examples of functional requests are military members asking to see their Military Personnel Records Jacket, or civilian employees asking to see their Official Personnel Folder.

2.5 Medical records
If it is determined that releasing medical information to the data subject could have an adverse effect on the mental or physical health of that individual, the requester will be asked to name a physician to receive the record. The data subject's failure to designate a physician is not a denial under the Privacy Act and cannot be appealed.

2.8 Fees
Requesters will be charged only for reproduction of requested documents. Normally, there will be no charge for the first copy of a record provided to an individual to whom the record pertains. Thereafter, fees will be computed as set forth in AR 34017.

2.9 Denial of access
a. The only officials authorized to deny a request from a data subject for records in a system of records pertaining to that individual are the appropriate AARAs, or the Secretary of the Army, acting through the General Counsel. (See para 17.) Denial is appropriate only if the record

(1) Was compiled in reasonable anticipation of a civil action or proceeding, or

(2) Is properly exempted by the Secretary of the Army from the disclosure provisions of the Privacy Act(see chap 5), there is a legitimate governmental purpose for invoking the exemption, and it is not required to be disclosed under the Freedom of Information Act.

b. Requests for records recommended to be denied will be forwarded to the appropriate AARA within 5 workdays of receipt, together with the request, disputed records, and justification for withholding. The requester will be notified of the referral.

c. Within the 30 workday period, the AARA will give the following information to the requester in writing if the decision is to deny the request for access: (See para 2-2.)

(1) Official's name, position title, and business address.

(2) Date of the denial.

(3) Reasons for the denial, includeing citation of appropriate sections of the Privacy Act and this regulation.

(4) The opportunity for further review of the denial by the General Counsel, Office of the Secretary of the Army, The Pentagon, WASH DC 20310-0104, through the AARA within 60 calendar days. (For denials made by the Army when the record is maintained in one of OPM's Government-wide systems of records, notices for which are described in AR 340-21-8, appendix A, an individual's request for further review must be addressed to the Assistant Director for Agency Compliance and Evaluation, Office of Personnel Management, 1900 E Street, NW, WASH DC 20415-0001.)

2.10 Amendment of records
a. Individuals may request the amendment of their records, in writing, when such records are believed to be inaccurate as a matter of fact rather than judgment, irrelevant, untimely, or incomplete.

b. The amendment procedures are not intended to permit challenges of an event in a record that actually occurred, or to permit collateral attack upon an event that has been the subject of a judicial or quasi-judicial action.

c. Consideration of a request for amendment would be appropriate if it can be shown that

(1) Circumstances leading up to the event recorded on the document were challenged through administrative procedures and found to be inaccurately described.

(2) The document is not identical to the individual's copy, or

(3) The document was not constructed in accordance with the applicable recordkeeping requirements prescribed.

d. For an example of c above, the amendment provisions do not allow an individual to challenge the merits of an adverse action. However, if the form that documents the adverse action contains an error on the fact of the record(for example, the individual's name is misspelled, or an improper date of birth or SSN was recorded), the amendment procedures may be used to request correction of the record.

e. USACIDC reports of investigation (records in system notices

A0501.08e Informant Register, A0508.11b Criminal Information Reports and Cross Index Card Files, and A0508.25a Index to Criminal Investigative Case Files) have been exempted from the amendment provisions of the Privacy Act. Requests to amend these reports will be considered under AR 195-2 by the Commander, U.S. Army Criminal Investigation Command. Action by the Commander, U.S. Army Criminal Investigation Command, will constitute final action on behalf of the Secretary of the Army under that regulation.

f. Records placed in the National Archives are exempted from the Privacy Act provision allowing individuals to request amendment of records. Most provisions of the Privacy Act apply only to those systems of records that are under the legal control of the originating agency; for example, an agency's current operating files or records stored at a Federal Records Center.

2.11 Procedures

a. Requests to amend a record should be addressed to the custodian or system manager of that record. The request must reasonably describe the record to be amended and the changes sought(that is, deletion, addition, or amendment). The burden of proof rests with the requester; therefore, the alteration of evidence presented to courts, boards, and other official proceedings is not permitted. (An individual acting for the requester must supply a written consent signed by the requester.)

b. The custodian or system manager will acknowledge the request within 10 workdays and make final responses within 30 workdays.

c. The record for which amendment is sought must be reviewed by the proper system manager or custodian for accuracy, relevance, timeliness, and completeness to assure fairness to the individual in any determination made about that individual on the basis of that record.

d. If the amendment is proper, the custodian or system manager will physically amend the record by adding or deleting information, or destroying the record or a portion of it. He or she will notify the requester of such action.

e. If the amendment is not justified, the request and all relevant documents, including reasons for not amending, will be forwarded to the proper AARA within 5 workdays; the requester will be notified.

f. The AARA, on the basis of the evidence, either will amend the record and notify the requester and the custodian or deny the request and inform the requester of--

(1) Reasons for not amending.

(2) His or her right to seek further review by the DA Privacy Review Board (through the AARA).

g. On receipt of an appeal from a denial to amend, the AARA will append any additional records or background information that substantiates the refusal or renders the case complete and, within 5 workdays of receipt, forward the appeal to the DA Privacy Review Board.

h. The DA Privacy Review Board, on behalf of the Secretary of the Army, will complete action on a request for further review within 30 workdays of its receipt by the AARA. The General Counsel may authorize an additional 30 days when unusual circumstances and good cause so warrant. The Board may seek additional information, including the appellant's official personnel file, if relevant and necessary to decide the appeal.

(1) If the Board determines that amendment is justified, it will amend the record and notify the requester, the AARA, the custodian of the record, and any prior recipients of the record.

(2) If the Board denies the request, it will obtain the General Counsel's concurrence. Response to the appellant will include reasons for denial and the appellant's right to file a statement of disagreement with the Board's action and to seek judicial review of the Army's refusal to amend.

i. Statements of disagreement will be an integral part of the record to which they pertain so the fact that the record is disputed is apparent to anyone who may have access to, use of, or need to disclose from it. The disclosing authority may include a brief summary of the Board's reasons for not amending the disputed record. The summary will be limited to the reasons stated to the individual by the Board.

2.12 Privacy case files

Whenever an individual submits a Privacy Act request, a case file will be established. (See system notice A0240.01DAAG.) In no instance will the individual's request and Army actions thereon be included in the individual's personnel file. The case file will comprise the request for access/amendment, grants, refusals, coordination action, and related papers. This file will not be used to make any determinations about the individual.

Chapter 3
Disclosure of Personnel Information to Other Agencies and Third Parties

3.1 Disclosure without consent

The Army is prohibited from disclosing a record from a system of records without obtaining the prior written consent of the data subject, except when disclosure is--

a. Made to officers and employees of DOD who have a need for the record in the performance of their duties.

b. Required under the Freedom of Information Act. (See para 3-3 for information normally releasable.)

c. Permitted by a routine use that has been published in the Federal Register.

d. Made to the Bureau of the Census for planning or carrying out a

census or survey, or to a related activity pursuant to title 13 of the United States Code.

e. Made to a recipient who has provided the Army with advance written assurance that the record will be--

(1) Used solely as a statistical research or reporting record.

(2) Transferred in a form that is not individually identifiable.

f. Made to the National Archives of the United States as a record that has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for determination of such value by the Administrator of the General Services Administration (GSA), or designee. (Records sent to Federal Records Centers for storage remain under Army control. These transfers are not disclosures and do not therefore need an accounting.)

g. Made to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if--

(1) The activity is authorized by law.

(2) The head of the agency or instrumentality has made a written request to the Army element that maintains the record. The request must specify the particular portion desired and the law enforcement activity for which the record is sought.

h. Made to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual. Upon such disclosure notification will be transmitted to the last known address of such individual.

i. Made to either House of Congress, or, to the extent of matter within its' jurisdiction, any committee or subcommittee thereof, any joint committee of Congress, or subcommittee of any such joint committee.

j. Made to the Comptroller General, or authorized representatives, in the course of the performance of the duties of the General Accounting Office(GAO).

k. Pursuant to the order signed by a judge of a court of competent jurisdiction. (Reasonable efforts must be made to notify the subject individual if the legal process is a matter of public record.)

l. Made to a consumer reporting agency under section 3(d) of the Federal Claims Collection Act of 1966(originally codified at 31 USC 952(d); recodified at 31 USC 3711(f)). The name, address, SSN, and other information identifying the individual; amount, status, and history of the claim; and the agency or program under which the case arose may be disclosed in this instance.

3.2 Blanket routine use disclosures

In addition to routine uses in each system notice, the following blanket routine uses apply to all records from systems of records maintained by the Army except those which state otherwise.

a. Law enforcement. Relevant records maintained to carry out Army functions may be referred to Federal, State, local, or foreign law enforcement agencies if the record indicates a violation or potential violation of law. The agency to which the records are referred must be the appropriate agency charged with the responsibility of investigating or prosecuting the violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

b. Disclosure when requesting information. A record may be disclosed to a Federal, State, or local agency that maintains civil, criminal, or other relevant enforcement information, or other pertinent information, such as licensing, to obtain data relevant to an Army decision concerning--

(1) Hiring or retention of an employee.

(2) Issuance of a security clearance.

(3) Letting of a contract.

(4) Issuance of a license, grant, or other benefit.

c. Disclosure of requested information. If the information is relevant and necessary to the requesting agency's decision, a record may be disclosed to a Federal agency in response to its request in connection with--

(1) Hiring or retention of an employee.

(2) Issuance of a security clearance.

(3) Reporting of an investigation of an employee.

(4) Letting of a contract.

(5) Issuance of a license, grant, or other benefit.

d. Congressional inquiries. Disclosure from a system of records maintained by the Army may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

e. Private relief legislation. Relevant information in all systems of records of DOD published on or before August 22, 1975, will be disclosed to OMB for review of private relief legislation, as set forth in OMB Circular A-19. Information may be disclosed at any stage of the legislative coordination and clearance process.

f. Disclosures required by international agreements. A record may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities. These disclosures are in compliance with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DOD military and civilian personnel.

g. Disclosure to State and local taxing authorities. Any information normally contained in Internal Revenue Service Form W-2, which

is maintained in a record from a system of records of the Army, may be disclosed to State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under 5 USC 5516, 5517, and 5520; only to those State and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use complies with Treasury Fiscal Requirements Manual, sec 5060.

h. Disclosure to OPM. A record may be disclosed to OPM concerning information on pay and leave, benefits, retirement deduction, and any other information necessary for OPM to carry out its legally authorized Government-wide personnel management functions and studies.

i. Disclosure to National Archives and Records Service (NARS), GSA. A record may be disclosed to NARS, GSA, in records management inspections conducted under 44 USC, 2904 and 2906.

j. Disclosure to the Department of Justice for litigation. A record may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing DOD, or any officer, employee, or member of DOD in pending or potential litigation to which the record is pertinent.

3.3 Disclosure to third parties

Personal information that may be disclosed under the Freedom of Information Act is as follows:

a. Military personnel.

(1) Name, rank, date of rank, gross salary, present and past duty assignments, future assignments that are officially established, office or duty telephone number, source of commission, promotion sequence number, awards and decorations, military and civilian educational level, and duty status at any given time.

(2) Lists or compilations of unit or office addresses or telephone numbers of military personnel are not released where the requester's primary purpose in seeking the information is to use it for commercial solicitation.

b. Civilian employees.

(1) Name and present and past position titles, grades, salaries, and duty stations that include office or duty telephone numbers.

(2) Disclosure of information in(1) above will not be made when the request is a list of present or past position titles, grades, salaries, and/or duty stations and--

(a) Is selected to constitute a clearly unwarranted invasion of personal privacy. For example, the nature of the request calls for a response that would reveal more about the employee than the items in(1) above.

(b) Would be protected from mandatory disclosure under an exemption of the Freedom of Information Act.

(3) In addition to the information in (1) above, the following information may be made available to a prospective employer of a current or former Army employee:

(a) Tenure of employment.

(b) Civil service status.

(c) Length of service in the Army and the Government.

(d) Date and reason for separation shown on SF 50 (Notification of Personnel Action).

3.4 Accounting of disclosure

a. An accounting of disclosure is required whenever a record from an Army system of records is disclosed to someone other than the data subject, except when that record--

(1) Is disclosed to officials within DOD who have a need for it to perform official business.

(2) Is required to be disclosed under the Freedom of Information Act.

b. Since the characteristics of records maintained within the Army vary widely, no uniform method for keeping the disclosure of accounting is prescribed. For most paper records, the accounting may be affixed to the record being disclosed. It must be a written record and consist of--

(1) Description of the record disclosed.

(2) Name, position title, and address of the person to whom disclosure was made.

(3) Date, method, and purpose of the disclosure.

(4) Name and position title of the person making the disclosure.

c. Purpose of the accounting of disclosure is to enable an individual--

(1) To ascertain those persons or agencies that have received information about the individual.

(2) To provide a basis for informing recipients of subsequent amendments or statements of dispute concerning the record.

d. When an individual requests such an accounting, the system manager or designee will respond within 10 workdays and inform the individual of the items in b above.

e. The only bases for not furnishing the data subject an accounting of disclosures are if disclosure was made for law enforcement purposes under 5 USC 552a(b)(7), or the disclosure was from a system of records for which an exemption from 5 USC 552a(c)(3) has been claimed. (See table 5-1.) AR 340-21 * 5 July 1985 * Unclassified

Chapter 4
Recordkeeping Requirements Under the Privacy Act

4.1 Systems of records

a. Notices of all Army systems of records are required by the Privacy Act to be published in the Federal Register. An example is at figure 4-1. When new systems are established, or major changes occur in existing systems, which meet the criteria of OMB guidelines summarized in paragraph 4-6b, advance notice must be furnished OMB and the Congress before the

system or proposed changes become operational.

b. Uncirculated personal notes, papers, and records that are retained at the author's discretion and over which the Army exercises no control or dominion are not considered Army records within the meaning of the Privacy Act. Individuals who maintain such notes must restrict their use to that of memory aids. Any disclosure from personal notes, either intentional or through carelessness, removes the information from the category of memory aids and the notes then become subject to provisions of the Act.

c. Only personal information that is necessary to accomplish a purpose or mission of the Army, required by Federal statute or Executive Order of the President, will be maintained in Army systems of records. Statutory authority or regulatory authority to establish and maintain a system of records does not convey unlimited authority to collect and maintain all information that may be useful or convenient. The authority is limited to relevant and necessary information.

d. Except for statistical records, most records could be used to determine an individual's rights, benefits, or privileges. To ensure accuracy, personal information to be included in a system of records will be collected directly from the individual if possible. Collection of information from third parties will be limited to verifying information for security or employment suitability or obtaining performance data or opiniontype evaluations.

4.2 Privacy Act Statement

a. Whenever personal information is requested from an individual that will become part of a system of records retrieved by reference to the individual's name or other personal identifier, the individual will be furnished a Privacy Act Statement. This State-ment is to ensure that individuals know why this information is being collected so they can make an informed decision on whether or not to furnish it. As a minimum, the Privacy Act Statement will include the following information in language that is explicit and easily understood and not so lengthy as to deter an individual from reading it:

(1) Cite the specific statute or Executive order, including a brief title or subject, that authorizes the Army to collect the personal information requested. Inform the individual whether or not a response is mandatory or voluntary and any possible consequences of failing to respond.

(2) Cite the principal purposes for which the information will be used.

(3) Cite the probable routine uses for which the information may be used. This may be a summary of information published in the applicable system notice.

b. The above information normally will be printed on the form used to record the information. In certain instances, it may be printed in a public notice in a conspicuous location such as at check-cashing facilities; however, if the individual requests a copy of its contents, it must be provided.

4.3 Social Security Number

Executive Order 9397 authorizes DA to use the SSN as a system to identify Army members and employees. Once a military member or civilian employee of DA has disclosed his or her SSN for purposes of establishing personnel, fiancial, or medical records upon entry into Army service or employment, the SSN becomes his or her identification number. No other use of this number is authorized. Therefore, whether the SSN alone is requested from the individual, or the SSN together with other personal information, the Privacy Act Statement must make clear that disclosure of the number is voluntary. If the individual refuses to disclose the SSN, the Army activity must be prepared to identify the individual by alternate means.

4.4 Safeguarding personal information

a. The Privacy Act requires establishment of proper administrative, technical, and physical safeguards to--

(1) Ensure the security and confidentiality of records.

(2) Protect against any threats or hazards to the subject's security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness.

b. At each location, and for each system of records, an official will be designated to safeguard the information in that system. Consideration must be given to such items as sensitivity of the data need for accuracy and reliability in operations, general security of the area, and cost of safeguards. (See AR 380-380.)

c. Ordinarily, personal information must be afforded at least the protection required for information designated "For Official Use Only." (See AR 340-17, chap IV.) Privacy Act data will be afforded reasonable safe-guards to prevent inadvertent or unauthorized disclosure of record content during processing, storage, transmission, and disposal.

4.5 First amendment rights

No record describing how an individual exercises rights guaranteed by the first amendment will be kept unless expressly authorized by Federal statute, by the subject individual, or unless pertinent to and within the scope of an authorized law enforcement activity. Exercise of these rights includes, but is not limited to, religious and political beliefs, freedom of speech and the press, and the right of assembly and to petition.

4.6 System notice

a. The Army publishes in the Federal Register a notice describing

each system of records for which it is responsible. A notice contains--

(1) Name and locations of the records.

(2) Categories of individuals on whom records are maintained.

(3) Categories of records in the system.

(4) Authority(statutory or executive order) authorizing the system.

(5) Purpose of the system.

(6) Routine uses of the records, including categories of users and purposes of such uses.

(7) Policies and practices for storing, retrieving, accessing, retaining, and disposing of the records.

(8) Position title and business address of the responsible official.

(9) Procedures an individual must follow to learn if a system of records contains a record about the individual.

(10) Procedures an individual must follow to gain access to a record about that individual in a system of records, to contest contents, and to appeal initial determinations.

(11) Categories of sources of records in the system.

(12) Exemptions from the Privacy Act claimed for the system. (See table 5-1.)

b. New, or altered systems that meet the requirements below require a report to the Congress and OMB. A new system is one for which no system notice is published in the Federal Register. An altered system is one that--

(1) Increases or changes the number or types of individuals on whom records are kept so that it significantly alters the character and purpose of the system of records.

(2) Expands the types or categories of information maintained.

(3) Alters the manner in which records are organized, indexed, or retrieved to change the nature or scope of those records.

(4) Alters the purposes for which the information is used, or adds a routine use that is not compatible with the purpose for which the system is maintained.

(5) Changes the equipment configuration on which the system is operated, to create potential for either greater or easier access.

c. Report of a new or altered system must be sent to HQDA(DAAG-AMR-S) at least 120 days before the system or changes become operational and include a narrative statement and supporting documentation. The narrative statement must contain the following items:

(1) System identification and name.

(2) Responsible official.

(3) Purpose of the system, or nature of changes proposed(if an altered system).

(4) Authority for the system.

(5) Number(or estimate) of individuals on whom records will be kept.

(6) Information on First Amendment activities.

(7) Measures to assure information accuracy.

(8) Other measures to assure system security. (Automated systems require risk assessment under AR 380-380.)

(9) Relations to State /local government activities. (See fig 4-2.)

d. Supporting documentation consists of system notice for the proposed new or altered system and proposed exemption rule, if applicable.

4.7 Reporting requirements

a. The annual report required by the Privacy Act, as amended by Public Law 97-375, 96 Statute 1821, focuses on two primary areas:

(1) Information describing the exercise of individuals' rights of access to and amendment of records.

(2) Changes or additions to systems of records.

b. Specific reporting requirements will be disseminated each year by HQDA(DAAG-AMR-S) in a letter to reporting elements.

4.8 Rules of conduct

Systems managers will ensure that all personnel, including Government contractors or their employees who are involved in the design, development, operation, maintenance, or control of any system of records are informed of all requirements to protect the privacy of individuals who are subjects of the records.

4.9 Judicial sanctions

The Privacy Act has both civil remedies and criminal penalties for violations of its provisions.

a. Civil remedies An individual may file a civil suit against the Army if Army personnel fail to comply with the Privacy Act.

b. Criminal penalties A member or employee of the Army may be found guilty of a misdemeanor and fined not more than $5,000 for willfully--

(1) Maintaining a system of records without first meeting the public notice requirements of publishing in the Federal Register.

(2) Disclosing individually identifiable personal information to one not entitled to it.

(3) Asking for or getting another's record under false pretenses.